Federal Public Key Infrastructure Policy Authority (FPKIPA)

Minutes of the 12 July 2005 Meeting

GSA; 1800 F Street; Room 5141B; Washington, DC

A. AGENDA

1) Welcome & Opening Remarks / Introductions
2) Discussion / Vote on Minutes from 14 June meeting
3) Government of Canada Trip Report
4) Change to Certificate Profile to simplify path discovery
5) Discussion/Vote on Draft Bylaws Document
6) Discussion of Audit Cycle Review Issues
7) Discussion on the New FBCA Policy Review
8) FPKI Certificate Policy Working Group (CPWG) Reports
9) FPKI Operational Authority (FPKI OA) Report
10) Final Meeting Items
11) Adjourn Meeting

B. ATTENDANCE LIST

VOTING MEMBERS

Organization	Name	Email	Telephone
Department of Commerce (NIST)	Polk, Tim		
Department of Defense	Hanko, Dave		
Department of Energy	ABSENT		
Department of Health & Human Services	Alterman, Peter		
Department of Homeland Security	ABSENT		
Department of Justice	Morrison, Scott		
Department of State	ABSENT		
Department of the Treasury	Moldenhauer, Michelle		
GSA	Temoshok, David		
NASA	DeYoung, Tice		
OMB	ABSENT		
USDA/NFC	Sharp, Kathy		
USPTO	Purcell, Art		

OBSERVERS

Organization	Name	Email	Telephone
NIST	Cooper, David		
Department of Homeland Security	Shomo, Larry		
General Services Administration	Duncan, Steve		
EDUCAUSE	Worona, Steve		
FICC Chair (GSA)	Spencer, Judith		
FICC Support (FC Business Systems)	Petrick, Brant		
Department of State (Mantech)	Froehlich, Charles		
FPKI OA (Mitretek)	Tate, Darron		
FPKI OA (GSA)	Jenkins, Cheryl		

Treasury Support (eValid8)	Dilley, Brian		
Department of Defense	Mitchell, Debbie		
USDA/NFC	Maldonado, Diana		
USDA/NFC	Morgan, Sheila		
State of Illinois	Anderson, Mark		

C. MEETING ACTIVITY

Agenda Items 1 & 2

Welcome & Opening Remarks / Introductions
Discussion / Vote on Minutes from 14 June meeting
This meeting took place at the GSA Central Office Building, 1800 F Street, Washington, DC in Room 5141B. Dr. Peter Alterman, Department of Health & Human Services (HHS) and FPKIPA Chair, called the meeting to order at 9:35 a.m. with attendee introductions.

The following table shows the votes recorded for the June 14, 2005 FPKIPA meeting minutes.

Approval vote for June 14, 2005 FPKIPA meeting minutes			
Voting members	**Vote (Motion – GSA; 2nd – DOC)**		
	Yes	**No**	**Abstain**
Department of Commerce	X		
Department of Defense	X		
Department of Energy	ABSENT – did not vote		
Department of Health & Human Services	X		
Department of Homeland Security	ABSENT – did not vote		
Department of Justice	X		
Department of State	ABSENT – did not vote		
Department of the Treasury	X		
GSA	X		
NASA	X		
OMB	ABSENT – did not vote		
USDA/NFC	X		
USPTO	X		

The June 14, 2005 FPKIPA meeting minutes were voted on and approved by the FPKIPA voting members. These meeting minutes will be posted to the FPKIPA web site by COB July 13, 2005.

Agenda Item 3

Government of Canada Trip Report – Ms. Judith Spencer
Ms. Spencer was invited to attend a Trans-Atlantic Secure Collaboration Joint meeting. A few of the attendees included the DoD, the Government of Canada (GOC) PKI Program Office, Microsoft, Exostar and Lockheed Martin. Ms. Spencer briefed the attendees on Federal PKI initiatives and on FIPS PUB 201. In separate meetings with the Canadian FPKI counterparts, discussions centered on FIPS PUB 201, which the GOC is looking at adopting a similar program to perform credentialing of its government workers. Since the GOC has a renewed interest with the FPKI community, we're in the process of scheduling a meeting at a U.S. facility between U.S. government FPKI officials and Canadian government PKI officials in the January 2006 timeframe. The next meeting would be scheduled at a GOC facility in the summer of 2006.

Agenda Item 4

Change to Certificate Profile to simplify path discovery – Mr. David Cooper

The Federal PKI X.509 Certificate and CRL Extension Profile was updated several years ago and is being updated to discourage users from implementing what the FBCA can't process. Entities that are cross-certified with the FBCA need to issue certificates in accordance with our new profile. Entities using well-connected directories do not have to tear down their existing infrastructure to accommodate AIA/SIA, but should begin working toward the future structure. Entities should be prepared to issue both segmented and full CRLs.

The DoD commented on the PIV authentication key and the card authentication key that is discussed in FIPS PUB 201. NIST will add these keys to the Federal Common Policy profile. The DoD wants 384-bit elliptic curves/SHA added as an option to the algorithms and key sizes in the Federal PKI profile. Specialized communities within the DoD use 384-bit elliptic curves/SHA.

The NIST wants to add a caveat so that smaller agencies don't spend their resources to support 384-bit elliptic curve. DISA comments recommended that HTTP be mandatory and that LDAP be optional. The current Federal PKI architecture has LDAP mandatory and HTTP optional. We'll vote on the updated Federal PKI X.509 Certificate and CRL Extension Profile at the next FPKIPA meeting (August 9, 2005). Dr. Alterman wants to make sure that the Department of State is involved and has reviewed this updated profile before it's voted on.

Agenda Item 5

Discussion / Vote on Draft Bylaws Document – Dr. Tice DeYoung and Mr. Charles Froehlich

Dr. DeYoung and Mr. Froehlich drafted the "By-Laws and Operational Procedures and Practices of the Federal PKI Policy Authority" document. Dr. Peter Alterman emailed the revised document to the FPKIPA members for their comments. Some of the comments received included procedures to handle grand-fathering of policies, an annual audit requiring to re-certify with the FBCA Certificate Policy (CP), to clarify the scope of the compliance audit requirements, election of the chair, term years for the chair, and removal of the chair.

Mr. Tim Polk would like to see both the FPKIPA By-Laws and the FPKIPA Charter as a package set and that both documents need to agree with each other. The FPKIPA members concurred and would like to see Dr. DeYoung and Mr. Froehlich map both of these documents to make sure they align correctly. The FPKIPA members agreed to postpone the vote on the By-Laws document.

Agenda Item 6

Discussion of Audit Cycle Review Issues –
Ms. Cheryl Jenkins, Ms. Kathy Sharp, and Mr. Dave Hanko

The proposed audit cycle for the FPKIPA will consist of three steps performed over a period of three consecutive years and then repeated. The initial phase will consist of an applicant that must complete an audit of their system records and activities in order to ensure compliance with their established policy and operational procedures, as a part of the FBCA cross-certification. The assessment must be performed by an external qualified third-party. The third-party must submit the applicant's assessment outcome in writing to the FPKIPA. The follow-on phase (the second year of being cross-certified with the FBCA) will consist of an entity completing an independent review of their system records and activities to report any indicated changes in policy and procedures. The independent reviewer must submit the entity's changes including language and practices in the policy-mapping table used in their cross-certification. The policy-mapping table will be forwarded to the FPKI CPWG. If a major change happens in the follow-on phase, a full compliance audit will need to be performed. The renewal phase will consist of the entity repeating the initial phase since this is the third year in which the security controls for each major application would be audited according to OMB A-130.

The checklist needs to be completed before it is emailed to the FPKIPA members. The checklist consists of common audit findings. This could include those findings that required corrective action or further investigation/monitoring.

It was determined by the FPKIPA members that a completed proposal is needed before the FPKIPA members vote on modifying the audit review requirements in the FBCA CP.

Agenda Item 7

Discussion on the New FBCA Policy Review – Mr. Tim Polk

As a reminder, the new FBCA CP (RFC 3647 format) was emailed to the FPKIPA members for review and comments. The new FBCA CP will be voted on at the next FPKIPA meeting (August 9, 2005). The new FBCA CP (Draft version) has been posted to the FPKIPA web site.

Action Item: Mr. Brant Petrick needs to map the new DoD CP (RFC 3647 format) against the new FBCA CP (RFC 3647 format) using the general requirements mapping matrix and the high level of assurance mapping matrix. These mapping matrices will be discussed at the FPKI CPWG meeting on July 28, 2005.

Agenda Item 8

FPKI Certificate Policy Working Group (CPWG) Reports – Mr. Tim Polk

The FPKI CPWG determined that the Wells Fargo CP/CPS met all requirements for the Medium Commercial Best Practice with the exception of in-person identity proofing.

Based on the meetings, submitted documents, and discussions with Wells Fargo, the FPKI CPWG recommends that the FPKIPA members approve a policy mapping for the Wells Fargo PKI at the FBCA Basic level of assurance, which is sufficient for E-Authentication level 3.

The following table shows the votes recorded to accept the FPKI CPWG Certificate Policy Mapping Report for the Wells Fargo PKI.

Approval vote for the Certificate Policy Mapping Report for the Wells Fargo PKI			
Voting members	**Vote (Motion – DoD; 2nd – DOC)**		
	Yes	**No**	**Abstain**
Department of Commerce	X		
Department of Defense	X		
Department of Energy	ABSENT – did not vote		
Department of Health & Human Services	X		
Department of Homeland Security	ABSENT – did not vote		
Department of Justice	X		
Department of State (proxy)	X		
Department of the Treasury (proxy)	X		
GSA (proxy)	X		
NASA (proxy)	X		
OMB	ABSENT – did not vote		
USDA/NFC (proxy)	X		
USPTO	X		

The Certificate Policy Mapping Report for the Wells Fargo PKI was voted on and approved by the FPKIPA voting members.

Wells Fargo technical interoperability testing with the prototype FBCA was successfully completed last week. Ms. Cheryl Jenkins will email the Wells Fargo technical interoperability test report to the FPKIPA members and then request a vote for acceptance. However, the MOA still needs to be completed by the Wells Fargo legal staff. Per Dr. Peter Alterman, the Wells Fargo compliance audit was satisfactory. Once received, the FPKIPA members need to review the Wells Fargo compliance audit report and then vote on accepting it.

Boeing agreed to changes that we requested from the policy mapping exercise. We're still waiting to hear from Boeing confirming the changes to their CP.

At the next FPKIPA meeting (August 9, 2005), we're going to discuss a change proposal that adds a high level of assurance policy OID to the Federal Common Policy.

Agenda Item 9

FPKI Operational Authority (FPKI OA) Report – Ms. Cheryl Jenkins

We still need to agree on a context prefix for the Federal PKI architecture.

Ms. Jenkins would like the FPKI CPWG to review the procedures to cross-certify with the FBCA.

Wells Fargo has successfully completed technical interoperability testing with the prototype FBCA.

Agenda Item 10

Final Meeting Items

Once received, the FPKIPA members will need to vote electronically on the Wells Fargo technical interoperability test report.

Pertaining to HSPD-12, the facial image on the chip is optional and new OMB guidance will hopefully be sent out at the end of this month.

The next FPKIPA Meeting is scheduled for August 9, 2005 (9:30 AM to 12:00 PM) at the GSA Central Office Building located at 1800 F Street, Room # 5141A, Washington, DC.

Agenda Item 11

Adjourn Meeting
The meeting adjourned at 11:49 a.m.

D. CURRENT ACTION ITEMS

No.	Action Statement	POC	Start Date	Target Date	Status
048	Solicit participants with a real application to do business with Canada.	Judy Spencer, GSA	10 June 2003	13 Jan 2004 FPKIPA meeting	**Open**
057	Write a short paper that says from here forward the FBCA OA will limit FBCA acceptance testing to systems that demonstrate enhanced assurance through NIAP testing.	Tim Polk, NIST	8 July 2003 Updated – 9 Sept 2003	9 Dec 2003 FPKIPA meeting	**Open**
062	Define the NIAP certification requirement for future bridge membrane applications.	Tim Polk, NIST	9 Sept 2003	9 Dec 2003 FPKIPA meeting	**Open**
066	Develop text for the FPKIPA Charter regarding the sunset clause for voting members of the FPKIPA who are not cross certified members of the FBCA.	Tim Polk, NIST	18 Nov 2003	13 Jan 2003 FPKIPA meeting	**Open**
085	Test/evaluate the PKCS-12 usage issue and make a recommendation to the FPKIPA at a meeting in the near future.	Tim Polk, NIST	13 July 2004	12 October 2004 FPKIPA meeting	**Open**
096	Research and draft FPKIPA charter updates to address Bridge-to-Bridge Cross-Certification.	Dr. Tice DeYoung, NASA	12 Oct 2004	Jan 2005 FPKIPA meeting	**Open**
097	Research and draft FBCA Criteria & Methodology document updates to address Bridge-to-Bridge Cross-Certification.	Dr. Peter Alterman, HHS	12 Oct 2004	Jan 2005 FPKIPA meeting	**Open**
112	Update their MOA with the FBCA to reflect the new one-way certificate being issued for the period of January 2005 to January 2006.	DoD	11 Jan 2005	28 Feb 2005	**Open**
113	Prepare and route a new Letter of Authorization from the FPKIPA to the FPKI OA for this new one-way cross-certificate for the DoD PKI for the period of January 2005 to January 2006.	Mark Lentz, Booz Allen Hamilton	11 Jan 2005	31 Jan 2005	**Open**
131	Develop a Compliance Audit Report paper on this issue and report to the FPKIPA at the 14 June FPKIPA meeting.	Cheryl Jenkins, GSA Dave Hanko, DoD	12 Apr 2005	14 June 2005 FPKIPA meeting	**Open**

No.	Action Statement	POC	Start Date	Target Date	Status
132	The FBCA TWG will be tasked with determining the LOE and cost necessary to post the Common Policy CA certificate in the root store cache leading email vendor products and report their findings at a future FPKIPA meeting.	Cheryl Jenkins, GSA	12 Apr 2005	14 June 2005 FPKIPA meeting	**Open**